COMMISSIONERS:
ART GRAHAM, CHAIRMAN
LISA POLAK EDGAR
NATHAN A. SKOP
RONALD A. BRISÉ
EDUARDO E. BALBIS

STATE OF FLORIDA

INSPECTOR GENERAL
STEVEN J. STOLTING
(850) 413-6071
FAX: (850) 413-6339

Public Service Commission

December 16, 2010

Ms. Kathy DuBose, Staff Director
Joint Legislative Auditing Committee
111 W. Madison Street
Tallahassee, Florida 32399-1400

Dear Ms. DuBose:

Pursuant to Section 20.055(5)(h), Florida Statutes, enclosed is a copy of my report to the Commission Chairman on the corrective actions taken in response to Auditor General Report No. 2010-197, *Information Technology Operational Audit - Case Management System.*

If you have questions or require additional information, please advise.

Sincerely,

Steven J. Stolting
Inspector General

SJS:ld

Enclosure

Cc: Mr. Tim Devlin
Mr. Curt Kiser
Mr. Charles Hill
Mr. Lee Kissell
Ms. Ann Cole

State of Florida

Public Service Commission

CAPITAL CIRCLE OFFICE CENTER • 2540 SHUMARD OAK BOULEVARD
TALLAHASSEE, FLORIDA 32399-0850

-M-E-M-O-R-A-N-D-U-M-

DATE: December 16, 2010

TO: Art Graham, Chairman

FROM: Steven J. Stolting, Inspector General

RE: Status of Agency Actions Regarding Auditor General Report (OIG 10/11-18)

Pursuant to Section 20.055(5)(h), Florida Statutes, the Office of Inspector General is required to report to you regarding the status of the Commission's response to recommendations by the Auditor General six months after issuance of the audit report. In June 2010, the Auditor General issued their information technology operational audit of our Case Management System (CMS), containing seven findings and corresponding recommendations for corrective action. The following provides the original recommendation, our initial response, and summarizes our actions in response over the intervening six months and the current status of the recommendation.

Recommendation No. 1: User Identification and Authentication Controls – The Commission should continue its efforts to improve user identification and authentication controls. Specifically, the Commission should assign each system user a unique user ID, expand the scope of its network password policy, and enforce the policy for all users.

Initial Response: We agree that, when feasible, network administration tasks should be performed by staff utilizing unique and identifiable login credentials. We will implement unique login credentials for each system which supports this functionality.

For hardware and software with independent authentication controls, the PSC agrees to implement a written password policy similar to our network password policy. When feasible, the password policy will be enforced with automated software controls. Not all hardware and software with independent authentication controls has a mechanism to enforce the written policy.

While PSC management continues to believe that a 180-day password expiration best balances our needs for security while minimizing the impact of more frequent password changes on Commission staff, Commission management agrees to consider a reduced interval for password changes and will incorporate any changes determined necessary in the password policy.

Current Status: *PARTIALLY IMPLEMENTED. The Commission has implemented steps to ensure that network administration tasks are performed by staff utilizing unique and identifiable login credentials. Specific steps taken to address this recommendation include:*

- *For Symantec Backup Exec data backup and restore operations all members of the Information Technology Services (ITS) staff are now required to use individual login credentials. Individual credentials have been established and tested, and use of these credentials is now required in ITS SOP 1510.*

- *ITS has created and tested unique login credentials for our Dell EqualLogic SAN management application. SAN administrators are now required to use their unique login credentials for all SAN management tasks.*

- *ITS has created and tested unique login credentials (Microsoft Active Directory credentials) for our Fortinet firewalls. ITS SOP 1540 requires firewall administrators to use these unique login credentials for all firewall management tasks. These credentials conform to all complexity and password length requirements.*

- *Office of Commission Clerk users of the CMS "RAR Fax" computer are now required to use their unique login credentials (Microsoft Active Directory) for all CMS fax management tasks. The generic RAR Fax user is no longer available.*

The PSC password policy (SOP 1530) has been expanded to include the firewall management system and SAN management software. PSC management stated that they have reviewed the required intervals for password changes, and determined that the current 180-day password-expiration policy best balances the need for security with the burden on staff of more frequent password changes. However, these password change requirements are now being enforced for all members of the PSC staff.

OIG determined that, while this recommendation is "partially implemented," PSC management has made the determination not to implement certain controls as noted above and plans no further actions regarding these issues. We also examined additional specific measures recommended for this finding area communicated confidentially due to their sensitivity. We found that those recommendations had been fully addressed.

Recommendation No. 2: Management of Access Privileges – The Commission should establish more comprehensive procedures for managing network and CMS access privileges and address inaccuracies in the network access procedures. Additionally, the Commission should remove all unnecessary or inappropriate access privileges and ensure that all access privileges have been authorized in writing by the functional owner.

Initial Response: We agree and will continue to refine our written procedures to address inaccuracies and document the assignment and removal of network and CMS access privileges by the functional owner. This will include regularly scheduled reviews of assigned access privileges and appropriate adjustments to ensure that only authorized users have access to resources.

Current Status: *FULLY IMPLEMENTED. ITS has implemented SOP 1550 to formalize change requests for CMS access privileges. In addition, SOP 1550 includes a requirement for annual review of CMS access privileges.*

ITS management has reviewed existing network access procedures and updated them to ensure that they are accurate. In addition, CMS access privileges have been reviewed for all ITS staff and privileges have been removed where appropriate. Written procedures now require that all requests for access privilege changes must originate from the functional owner or designee.

Recommendation No. 3: Background Checks – The Commission should ensure that all employees in sensitive positions have undergone appropriate background checks. Additionally, the Commission should perform background checks on a periodic basis.

Initial Response: We agree and have obtained the necessary authorizations from law enforcement to perform such checks for all information technology staff. In addition, we are currently developing Commission policies to conduct background checks and require rechecks every three years.

Current Status: *FULLY IMPLEMENTED. On July 27, 2010, the Commission's Administrative Procedures Manual (APM 4.02-S) on background screening was amended to reflect the inclusion of Level 2 screening for all ITS staff. As of September 13, 2010, all ITS employees had completed their Level 2 screening. The policy requires that all ITS employees be rescreened every three years.*

Recommendation No. 4: Program Change Controls – The Commission should establish a comprehensive systems-development life-cycle methodology that includes the above-noted change control procedures and process to promote the ongoing integrity of CMS.

Initial Response: We agree and will implement a systems-development life-cycle methodology which includes the change control procedures noted in the finding.

Current Status: *PARTIALLY IMPLEMENTED. ITS management is in the process of implementing a systems-development life-cycle methodology which includes the cited change control procedures. Steps in this process include:*

- *ITS SOP 1412 has been updated to codify the process for submitting and documenting CMS programming change requests. The SOP requires all change requests to come from the program's functional owner and maintenance of copies of requests by the supervisor of the Custom Programming Section;*

- *Development currently underway of a written SOP to require control and documentation when program changes are moved into production. The pending SOP will move responsibility for approving the posting of new code into production from the application programmers to the supervisor of the Custom Programming Section.*

After completion of these steps, ITS management stated that they will then determine what additional measures are necessary to further implement a comprehensive systems-development life-cycle methodology.

Recommendation No. 5: Security Awareness Training – The Commission should promote security awareness through a comprehensive training program to ensure that all employees are aware of the importance of information in their possession and their responsibilities for maintaining its confidentiality, integrity, and availability.

Initial Response: We agree and have implemented annual training classes for all staff.

Current Status: *FULLY IMPLEMENTED. A program of annual training classes has been implemented applicable to all Commission staff.*

Recommendation No. 6: Network Security Controls and IT Disaster Recovery Planning Controls – The Commission should implement the appropriate network security controls and IT disaster recovery plan provisions to ensure the continued confidentiality, integrity, and availability of Commission data and IT resources.

Initial Response: We agree and will implement network security controls and IT disaster recovery plan provisions to address the cited finding issues.

Current Status: *PARTIALLY IMPLEMENTED. ITS management is in the process of addressing cited needs for improvement in security controls and IT disaster recovery plan provisions. We also examined recommended controls for this finding area communicated confidentially to ITS staff due to their sensitivity. Most of these have been fully addressed, but in a few cases, PSC management has declined to implement certain controls based either on the presence of alternative controls or the burdens of implementation on Commission operations versus the perceived risks.*

Recommendation No. 7: Communication Technologies – The Commission should continue its efforts to revise its Administrative Procedures Manual to provide the necessary guidance for these communication devices to Commission staff.

Initial Response: We agree and have developed revised procedures which should be adopted within the near future. In the interim, all functionality of these devices other than standard e-mail remains effectively disabled.

Current Status: *PARTIALLY IMPLEMENTED. The Commission is continuing to develop procedures to govem use of these devices. Additional consideration is being given to what uses are appropriate, incorporating necessary management controls and public records requirements. All functionality of these devices that does not meet these requirements continues to be disabled.*

We found that Commission management and staff have made significant efforts to address the report recommendations, and for areas remaining "partially implemented," processes have begun that require longer time periods to meet the requirements of the recommendation. In a few cases as noted above, management is considering alternative controls or acceptance of a cited risk where the impacts of fully implementing the recommendation on Commission operations were determined to be significant.

Based on this assessment, I have concluded that all corrective actions agreed to by management in response to these recommendations have been completed or are underway. My office will continue to monitor and assist in these activities as needed.

If you have any questions or need additional information, please feel free to contact me.

SJS:ld